PF020092
US

PCT World Intellectural Property Organization
International Office

International Application Published under the Patent Cooperation Treaty

(51) International Patent Classification[7]: **H04N 7/16, G10H 1/00**

(11) International Publication No. **WO 00/11867**

A1 (43) International Publication Date: 2 March 2000 (02.03.00)

(21) **International File No.**: PCT/FR99/02017

(22) **International Application Date**: 19 August 1999 (19.08.99)

(30) **Priority**:
90/10543 19 August 1998 (19.08.98) FR

(71) **Applicant** (*for all designated countries except US*):
INNOVATRON (SOCIETE ANONYME [FR/FR]; 1, rue Danton , F-75006 Paris (FR)

(72) **Inventors; and**
(75) **Inventors/Applicants** (*only for US*):
MORENO, Roland [FR/FR]; 3, rue de L'ancienne Comédie, F-75006 Paris (FR).

(74) **Representative:** DUPUIS-LATOUR, Dominique; Cabinet Bardehle, Pagenberg & Partner, 14 boulevard Malesherbes, F-75008 Paris (FR)

(81) **Designated States**: AE, AL, AU, BA, BB, BG, BR, CA, CN, CU, CZ, EE, GE, HR, HU, ID, IL, IN, IS, JP, KP, KR, LC, LK, LR, LT, LV, MG, MK, MN, MX, NO, NZ, PL, RO, SG, SI, SK, SL, TR, TT, UA,US, UZ, VN, YU, ZA, ARIPO Patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM) European Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG)

Published:
with international search report

[Abstract in English]

METHOD FOR CERTIFIED DELIVERY OF AN AUDIO, VIDEO OR TEXT SEQUENCE

The present invention concerns a method for delivery of audio, video, text or similar sequences to a remote site through downloading of data.

The invention will be described within the framework of audio sequences, since involved there is the most immediate application, taking into account the current capacities of the distribution networks; however, the invention can be directly transposed to the acquisition of other types of sequences, notably video data (television still or moving images) of text sequences. It can likewise be applied to the acquisition of sequences forming data processing files, for example data required for the downloading of software, or to allow the user to utilize software that necessitates an exchange of data with a remote site.

The sound reproduction machinery can function from various sources, such as recorded media (disks, tapes, etc.) or remotely transmitted sources (radio broadcasting, etc.).

These sources have various disadvantages:

- The use of recorded media presupposes that the user first has to buy or rent the media, with naturally all of the difficulties or problems that he or she may encounter whenever trying to obtain rare or old or difficult-to-find recordings;

- Radio-broadcasted sources by themselves have the drawback of a limited number of choices in the number of stations that can be picked up by the user, and the inability to choose the exact starting **observing** time, with the user furthermore being restricted to the broadcast times of the station whose signal he or she wants to receive.

Modern techniques of data compression today make it possible to transmit sound, particularly recorded music through a remote data processing network (for example an Internet network) under excellent technical conditions, i.e., conditions that are compatible with the highest degree of sound quality that is now available.

These possibilities are in particular available in the case of an "MP3" type of compression, with a rate of around 60,000 bps (bits per second), i.e., on the order of the speed available from currently available modems, with the data being decompressible in real time at hearing or observing speed. Even more favorable prospects can be envisaged with transmission of rates even higher than those provided over the RNIS network or over cable networks, or satellite transmission of digitized data over high-rate television channels.

These techniques combine a great number of advantages:

- A vast choice of selections (e.g., musical pieces);
- Ability to select immediately from the time of installation;
- Ability to choose the precise time when one wants to observe;
- Absence of any recorded media (thus a space-saving benefit and less cost for equipment because of the absence of mechanical elements);
- Digital type sound quality, namely greatly superior to that offered by broadcasting.

The invention concerns more particularly the payment of broadcast or distribution royalties depending on the choice made by the user, in the same way as in the case of a purchase of magnet media.

The purpose of the invention is to offer a secure method for the payment of these royalties that allow for countering any attempts at fraud, such as downloading without

payment of royalties or unauthorized reproduction of sequences.

The invention also concerns the distribution of these royalties among the various music publishers, and looks to avoid the disadvantages and drawbacks of payment of royalties by broadcasters, who account for these royalties approximately but not statistically in terms of the real or actual audience at the time when such musical selection is broadcast.

More precisely, according to one of these aspects, the present invention concerns a method for the delivery of audio, video or text sequences to user equipment co-operating with a microcircuit, notably a chip card microcircuit, by remote transmission of digital data representative of these sequences, which method comprises stages including:

- Connecting the apparatus to a remote server;
- Issuing a request to this server for the choice of sequence;
- Receiving in response from this server a flow of compressed and encrypted digital signals corresponding to the sequence chosen;
- Decompressing and decrypting the received flow and transforming it into an audio, video or text signal that can be reproduced and presented for the user,

this method being characterized in that it also embodies the following stages:

- Entry of debit information pertaining to the chosen sequence into the memory of the microcircuit;
- Transmission of debit information to a remote payment site, whether or not different from that of the server;

- Generating of an appropriate cryptographic certificate by the payment site;

- Transmission of said cryptographic certificate to the apparatus;

- Verification by the apparatus of the conformity of said cryptographic certificate;

- In case of acknowledged conformity, delivery of the data of said audio, video or text signal ready to be reproduced and given to the user in decompressed and decrypted form.

There are also several advantageous subsidiary methods of implementation, to wit:

- The certificate is an intrinsic certificate, the function of which is the cryptographic key that allows for the decoding;

- Information about the holder of the royalties is combined with the sequence information, and the payment site sends the respective holders of the royalties the payments corresponding to the selected sequences;

- The method furthermore embodies a stage that provides for the inclusion, through the microcircuit, of a watermark in the audio, video or text signal that can be reproduced and presented to the user, this watermark embodying an identifier of the microcircuit;

- The data from the audio, video or text signal are, at the choice of the apparatus user, delivered in analog or else digital form, and the debit information is differentiated depending on this choice.

According to a second aspect of the invention, it addresses a method for delivering audio, video or text sequences to a user apparatus that operates with a

microcircuit, notably a chip card microcircuit, by remote transmission of digital data representing these sequences, which method comprises stages including:

a) Connecting the apparatus to a remote server;
b) Sending this server a request for choice of sequence;

c) Receiving in response from this server a flow of compressed and encrypted digital signals corresponding to the sequence chosen;

d) Entering debit information pertaining to the chosen sequence into the memory of the microcircuit ;

e) Decompressing and decrypting the received flow and transforming it into an audio, video or text signal that can be reproduced and presented to the user,

with this method being characterized in that during stage e), the decrypting is achieved through means that include said microcircuit used for operating stage d), i.e., the entry of the debit information.

Furthermore, the method has the advantageous characteristic of having a stage that provides for the inclusion, through the microcircuit, of a watermark in the audio, video or text signal that can be reproduced and presented to the user, this watermark embodying an identifier of the microcircuit.

<>

The following comprises a description of one example of the embodiment of the invention, with reference to the appended drawings.

Figure 1 is a function block diagram showing the different components of a piece of equipment or apparatus that allows for the implementation of the invention.

Figure 2 is a block diagram showing a variant of Figure 1, with a superior degree of integration of the components.

Figure 3 illustrates the exchanges of signals between the different sites or blocks participating in the implementation of the method according to the present invention.

<>

In Figure 1, reference 10 indicates a classical amp/pre-amp stereo unit that supplies the output to a pair of speakers 12. The unit 10 can be either integrated into the rest of the apparatus (which is presented in an external view and is in the traditional mode of a hi-fi amplifier) or can be separate from the apparatus (the apparatus is then in the form of a case or box of the same type as a CD player, tuner, etc., connected to one of the inputs of a traditional amplifier).

It should be noted that the apparatus can also be structured in the form of a dedicated apparatus (as described here), like an extension to a microprocessor, in other words it may be made up of only a microprocessor combined with a chip card reader.

The apparatus includes a display 14 that presents the user with a series of musical selections, as well as the tools to choose these musical selections, for example in the form of a small wheel 16 (in order to scroll the selections), combined with a validation button 18.

The apparatus likewise embodies a programmable processor 20, composed essentially of a central processing unit CPU 22 and non-volatile storage MNV 4 [*sic:* 24], irrespective of its own ROM 26 and RAM 28 memory resources. The processor 20 receives the selection and validation data from the wheel 16 and the button 18, and it drives the display 14.

The non-volatile memory 24 might also embody a low-volume hard disk, if special technical limitations make this necessary, or it may be composed simply of a "solid disk", that is, a large-dimensioned semi-conductor memory, for example 32 Mb.

The apparatus is also connected to a modem 30 which allows the apparatus to interface with the telephone network 32, typically at a speed of 56,000 bps.

The apparatus also embodies a switching circuit 34 allowing one to select reception both from a radio source through the modem 30 and the other traditional amplifier input media (CD, tuner, cassette, etc.), combined in the drawing as an auxiliary input 36.

The processor 20 is moreover connected to a chip card 38, the role of which will be explained later on, through the intermediary of a reader 40.

The use of this apparatus is essentially as follows:

Upon powering up, for example using the button 18, the apparatus automatically connects via the telephone network 32 to a remote site or to a "sound recording library", whose Internet or other address is permanently recorded in the non-volatile memory 24.

The main program driving the processor 20 then allows "navigation" at this site; this program embodies for example a sub-assembly or sub-group of traditional navigation software, specially adapted to and simplified for the needs of the device according to this invention.

Thus, the user will be able to navigate through a repertory of musical selections, which he or she will be able to scroll through and select by using the wheel 16 and the button 18.

If necessary and/or appropriate, the navigation system and the display can be adapted so as to facilitate access by selection of musical genres and sub-genres, or further still by crossed selection between musical genres (classical, jazz, opera, etc.) and type of works (original editions, novelties, high-demand and low-demand titles, etc.). The display 14 may then be configured in the form of a double-entry panel with

selection options by appropriate commands using a touch screen or a double row of buttons, etc., allowing for a configuration in the form of a line/column intersection.

Once the choice of the musical selection has been made, the processor 20 sends a command to the remote site so as to allow the downloading of the musical selection chosen.

This downloading can be done in real time (oberving simultaneously with the downloading) or quasi-real time, by providing the processor with a buffer storage in order to increase decompression and/or decrypting performance.

The chip card 38 is used for decrypting purposes and possibly for payment of the royalties on the musical work selected by the user.

It can be used also advantageously in a structure like that shown in Figure 2, showing an enhanced degree of integration and thus provide greater anti-fraud security.

The security/decrypting/payment circuits are included in a block 42, advantageously embodied in the form of a single integrated assembly, integrated circuit or hybrid circuitry embedded in protective material that impedes any non-destructive access to the circuit components.

This block 42 embodies a microcircuit 44 that receives the identifying information 52 from the raw flow (that is, encrypted and compressed) via the modem 30 and is loaded to generate the keys 48 required for decrypting, and comprised typically via the microcircuit of a chip card. As a variant, it can be composed of a so-called SAM-type module (Security Access Module), and possibly combined with other SAM modules in the decoder.

The block 42 also embodies a decrypting module 50 that receives the musical information 52 from the raw flow coming from the modem 30, and processes it through keys 48 in order to deliver an decrypted and compressed output flow 54. Furthermore,

the block 42 embodies a decompression module 56, for example of the MP3 type, at 44.1 kHz, 16 bits stereo, at a rate compatible with real time observing, delivering as output a flow of decrypted and decompressed data 58 sent to the input of the amplifier 10.

In a variant of the embodiment according to the invention, a digital output of the data is provided, advantageously in a prescribed standardized format, such as the SDMI (Secure Digital Music Initiative) format, the specifications of which are published at the Internet site www.sdmi.org). This format can embody an identifier, advantageously coming from a chip card, and moreover the payment of the royalties may be different depending on whether or not this digital output is activated.

In a particularly advantageous embodiment, it is this same card 38 which serves not only for decrypting purposes, but also for the payment of the royalties due on the musical work. This payment may be made through known software methods such as "cybercash", "virtual money", etc.

The data that has to be exchanged in order to allow payment are illustrated schematically in Figure 3.

This method of payment implies exchanges of signals between the following points:

- "Music" site SM, which is an Internet site for the publisher of the musical selection chosen;
- "Corporate" site SC, common to various publishers participating in the system and responsible for distributing income from royalties among these publishers;
- Non-volatile memory MNV of the apparatus for the temporary storage of data;
- Apparatus software SOFT;
- Chip card 38
- Amplifier 10.

The different stages referenced 1 to 7 in the Figure are the following:

1. The music site SM corresponding to the selection chosen by the user sends an MP3 file or a block of MP3 data to the apparatus, which stores this information in its non-volatile memory.
2. The exchange of data between the apparatus and the chip card (flow 2 and 2') performs an initial decoding of the data in block 50 shown in Figure 2.

3. The apparatus then enters the debit information in the memory of the chip card corresponding to the chosen selection and the publisher of the music.

4. The apparatus is connected to the corporate site CS; the debit information stored in stage 3 is then transmitted to the corporate site, which issues a cryptographic certificate.

5. This cryptographic certificate is transmitted to the decoder, which verifies its conformity, and if such is the case, authorizes the delivery (phase 6 below) of the decompressed and decrypted data.

6. Conditionally (see stage 5 above), the software delivers the decompressed and decrypted data to the amplifier for observing;

7. At regular intervals, the corporate site credits the particular music publishers for the royalties debited in the apparatus.

The verification of the cryptographic certificate at phase 7 can be done by the chip card itself, or optionally by a separate SAM circuit. Furthermore, in a particular mode of embodiment, the certificate can be an intrinsic certificate, i.e., of which it is the function of the cryptographic key to allow the decoding of the data to be observed.

The debiting may be done by various known means: use of a pre-paid card, a subscription card that can debit the subscriber at a later time, for example, on the invoice that the subscriber receives from his or her Internet provider, including an

honor system for free promotional selections, etc.

The payment method can be summarized by the following metalanguage algorithm:

Amplifier:

while counter > Max
Exec (Payment_Process)
Exec (Receive_New_Key)
wend
Exec (Pay_Then_Decode)
END

Remote site:

Receive_Card_Counter
while counter > Max
Exec (Payment_Process)
wend
Download_Music
return

Payment process (amplifier):

Payment_Process_Protocol
if payment is NOT OK **then END**
Receive_New _Key
return

Payment process (remote site):

Receive_Royalties_Data from Card
if Royalties_Data is NOT OK **then END**
Debit_Customer_Royalties_Sum

Credit_Publisher
Send **New** Key
set Card_Counter = 0
return

Furthermore, in a variant of the embodiment according to this invention, the cryptographic possibilities offered by the combination of three particular datum (or source of data) may be utilized:

- Identification card;
- Exploitation data (digitized music);
- Random seed (regular or periodical).

Thus, modulation can be made dependent upon the identity of the amplifier-client, in other words non-decodable by an intruder who is improperly looking to decode the musical selections that are not intended for him or her. Furthermore, such a device would permit the establishment of rates proportional to the observing time, provided that the periodicity of the random seed is sufficiently brief. For example: one counting unit every sixty seconds.

In one particular embodiment, it is possible to provide for the inclusion of a "watermark" in the data flow.

The technique of including a "watermark" or a "tattoo" is in and of itself known, and is described in Petitcolas *et al.*, Information Hiding - A Survey, *Proceedings of the IEEE*, 87(7): 1062 - 1078, July 1999, or Boney *et al.*, Digital Watermarks for Audio Signals, *European Signal Processing Conference, EUSIPCO 96*, Trieste, Italy, September 1996, as well as in US-A 5,828,315; US-A 5,613,004; US-A 5,687,191 and US-A 5,822,360, or in the presentation of the *Musicode* system of Aris Technologies (www.musicode.com) and *Audiomark* of Alpha Tec Ltd. (www.alphatecltd.com).

The invention however offers the embodiment:

- At the music site, of "watermarking" or "tattooing" the coded data flow (compressed and coded) sent to the user, and/or

- At the decoder, locally and within the chip card itself during the decrypting and decompression operations, of "watermarking" or "tattooing" the decrypted and decompressed output data flow, with the watermarking incorporating an identifier of the card used for the decrypting and decompression of these data.

Generally speaking, this technique is comprised of adding inaudible information to the musical message, which information can be revealed by appropriate methods.

For an analog signal, the simplest technique combines the addition of a low level identifying signal coding the identifying information in a highly redundant manner, for example, by adding a 10 kHz carrier that is inaudible in relation to the musical message and in-phase modulated to 100 bits/second; the disclosure is done through filtering techniques with correlation. For a digital signal, operations of the same nature may be undertaken digitally. More simply, the identification message can be multiplexed with the original message and with the sound reproduction ignored (but in this case the identifying message can be easily removed).

Numerous techniques exist for making the watermarking or tattooing undetectable, or difficult to remove or mask, and slightly altering the message. Certain techniques allow for tattooing or watermarking the compressed music digitally without even decompressing it, which is well suited in the case of the invention.

CLAIMS

1. Method for the delivery of audio, video or text sequences to the user apparatus or equipment, co-operating with a microcircuit (44), notably a chip card microcircuit (38), by remote transmission of digital data representing these sequences, with said method comprised of stages including:

- Connecting the apparatus to a remote server;
- Issuing a request to this server for the choice of sequence;
- Receiving in response from this server a flow of compressed and encrypted digital signals corresponding to the sequence chosen;
- Decompressing and decrypting the received flow and transforming it into an audio, video or text signal that can be reproduced and shown to the user,

this method being characterized in that it also embodies the following stages:

- Entry of debit information pertaining to the chosen sequence into the memory of the microcircuit;
- Transmission of debit information to a remote payment site, whether or not different from that of the server;
- Generation of an appropriate cryptographic certificate by the payment site;
- Transmission of said cryptographic certificate to the apparatus;

- Verification by the apparatus of the conformity of said cryptographic certificate;

- In case of acknowledged conformity, delivery of the data of said audio, video or text signal ready to be reproduced and given to the user in decompressed and decrypted form.

2. Method according to claim 1, in which the certificate is an intrinsic certificate, the function of which is the cryptographic key that allows for the decoding;

3. Method according to claim 1, in which information about the holder of the royalties is combined with the sequence information, and in which the payment site sends the respective holders of the royalties the payments corresponding to the selected sequences.

4. Method according to claim 1, furthermore embodying a stage that provides for the inclusion, through the microcircuit, of a watermark in the audio, video or text signal that can be reproduced and presented to the user, this watermark embodying an identifier of the microcircuit.

5. Method according to claim 1, in which data from the audio, video or text signal are, at the choice of the apparatus user, delivered in analog or else digital form, and in which the debit information is differentiated depending on this choice.